

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-138671

(43) Date of publication of application : 16.05.2000

(51) Int. Cl.	H04L 9/32
	G06F 17/60
	G06T 7/00
	G09C 1/00
	G09C 5/00

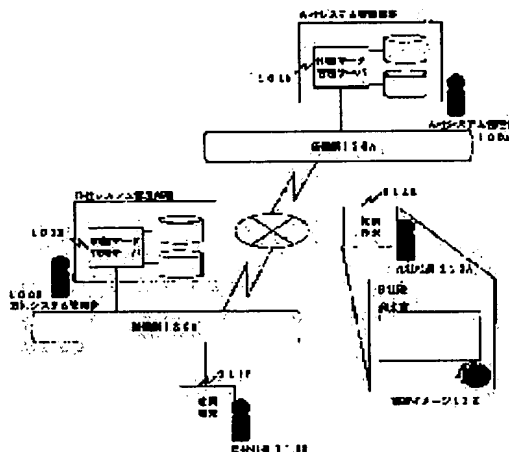
(21)Application number : 10-309806 (71)Applicant : HITACHI LTD
(22)Date of filing : 30.10.1998 (72)Inventor : TSUCHIYAMA CHIKAKO
TOYOSHIMA HISASHI
NAGAI YASUHIKO

(54) ELECTRIC SEAL MARK AUTHENTICATION

(57) Abstract:

PROBLEM TO BE SOLVED: To identify a correct person and data at the time of transmitting and receiving digital data by adding a mark in which personal identification information and digital data authentication information are included in a mark design to digital data so as to authenticate digital data through the use of authentication information in the mark.

SOLUTION: A clerk terminal 111A displays digital data with a seal mark stuck to it. When a clerk 110A clicks the authentication button of the seal mark, the authentication item section of the seal mark is displayed. When the clerk 110A clicks the personal authentication item of the seal mark, a seal mark authentication processing part extracts personal authentication information from the seal mark. It is collated whether an open key for decoding extracted personal authentication information matches with an open key stored in the terminal 111, etc. When it matches, a seal mark authentication processing part displays personal authentication information in a processing picture image so as to confirm contents by decoding personal information extracted from the seal mark and authenticates.



LEGAL STATUS

[Date of request for examination] 26.08.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of

BEST AVAILABLE COPY

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2000-138671

(P2000-138671A)

(43)公開日 平成12年5月16日(2000.5.16)

(51)Int.Cl. ⁷	識別記号	F I	テーマコード [*] (参考)
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 D 5 B 0 4 3
G 0 6 F 17/60		C 0 9 C 1/00	6 6 0 B 5 B 0 4 9
G 0 6 T 7/00		5/00	5 J 1 0 4
G 0 9 C 1/00	6 6 0	C 0 6 F 15/21	Z
5/00		15/62	4 5 5

審査請求 未請求 請求項の数10 O L (全 18 頁) 最終頁に続く

(21)出願番号 特願平10-309806

(22)出願日 平成10年10月30日(1998. 10. 30)

(71)出願人 000003108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72)発明者 土山 千佳子

神奈川県川崎市幸区鹿島田890番地 株式会社日立製作所システム開発本部内

(72)発明者 豊島 久

東京都江東区新砂一丁目6番27号 株式会社日立製作所公共情報事業部内

(74)代理人 100083552

弁理士 秋田 収喜

最終頁に続く

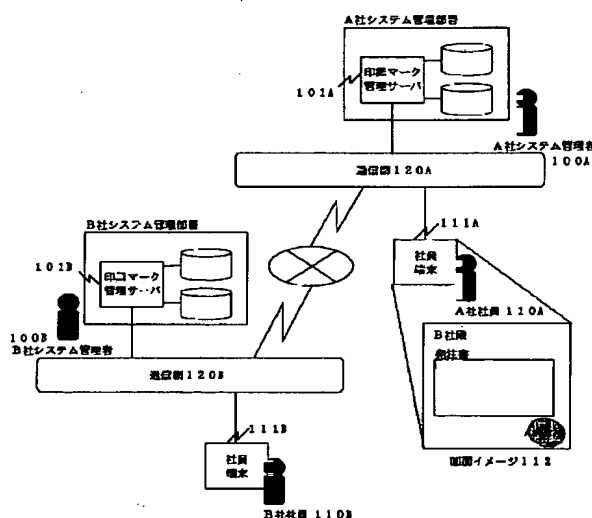
(54)【発明の名称】 電子印鑑マーク認証システム

(57)【要約】

【課題】 ネットワーク上でデジタルデータを送受信する際の本人認証及びデータ認証を実現することが可能な技術を提供する。

【解決手段】 印影または署名を表すマークによりデジタルデータの認証を行うマーク管理サーバにおいて、マークの新規登録または更新を要求するマーク登録要求をマーク端末装置から受信し、要求元の人物を認証する為の情報を暗号鍵で暗号化した本人認証情報を当該要求元のマークデザインに埋め込んでマークを作成し、前記作成したマークに前記本人認証情報を復号化する為の復号鍵を添付して要求元に配布するマーク管理処理部と、前記暗号化した本人認証情報を復号化する為の復号鍵をマーク復号鍵管理DBに登録し、前記登録した復号鍵を各マーク端末装置に送信するマーク復号鍵管理処理部とを備えるものである。

図1



(2) 000-138671 (P2000-138671A)

【特許請求の範囲】

【請求項1】 印影または署名を表すマークによりデジタルデータの認証を行うマーク管理サーバにおいて、マークの新規登録または更新を要求するマーク登録要求をマーク端末装置から受信し、要求元の人物を認証する為の情報を暗号鍵で暗号化した本人認証情報を当該要求元のマークデザインに埋め込んでマークを作成し、前記作成したマークに前記本人認証情報を復号化する為の復号鍵を添付して要求元に配布するマーク管理処理部と、前記暗号化した本人認証情報を復号化する為の復号鍵をマーク復号鍵管理DBに登録し、前記登録した復号鍵を各マーク端末装置に送信するマーク復号鍵管理処理部とを備えることを特徴とするマーク管理サーバ。

【請求項2】 前記マーク管理処理部は、本人認証情報が埋め込まれていることを示す視認性を可視透かしにより前記マークに持たせることを特徴とする請求項1に記載されたマーク管理サーバ。

【請求項3】 前記マーク管理処理部は、マーク付加時に送信されるログ情報をマークログ管理DBに格納するものであることを特徴とする請求項1または請求項2のいずれかに記載されたマーク管理サーバ。

【請求項4】 印影または署名を表すマークによりデジタルデータの認証を行うマーク端末装置において、マークの新規登録または更新を要求するマーク登録要求をマーク管理サーバに送信し、要求元の人物を認証する為の情報を暗号鍵で暗号化した本人認証情報を当該要求元のマークデザインに埋め込んで作成したマークをマーク管理サーバから受け取るマーク登録処理部と、本人認証情報を復号化する為の復号鍵をマーク管理サーバから受信し、前記復号鍵を復号鍵DBに格納する復号鍵格納処理部とを備えることを特徴とするマーク端末装置。

【請求項5】 印影または署名を表すマークによりデジタルデータの認証を行うマーク端末装置において、マークが付加されるデジタルデータの特徴情報を含むデジタルデータ認証情報とマーク付加通算番号とをユーザ固有の暗号鍵で暗号化し、本人認証情報が埋め込まれたマークに前記暗号化されたデジタルデータ認証情報及びマーク付加通算番号を埋め込み、前記デジタルデータの選択された位置に前記マークを付加するマーク付加処理部を備えることを特徴とするマーク端末装置。

【請求項6】 前記マーク付加処理部は、デジタルデータ認証情報が埋め込まれていることを示す視認性を可視透かしにより前記マークに持たせることを特徴とする請求項5に記載されたマーク端末装置。

【請求項7】 前記マーク付加処理部は、マーク付加時にログ情報をマーク管理サーバに送信するものであることを特徴とする請求項5または請求項6のいずれかに記載されたマーク端末装置。

【請求項8】 印影または署名を表すマークによりデジ

タルデータの認証を行うマーク端末装置において、デジタルデータに付加されたマークから本人認証情報を抽出し、その本人認証情報を復号化する為に添付された復号鍵が復号鍵DBに格納されている復号鍵と合致するかどうか照合し、前記復号鍵が合致している場合には前記マークから抽出した本人認証情報を前記復号鍵で復号化して本人認証情報を表示し、合致していない場合にはエラーメッセージを表示するマーク認証処理部を備えることを特徴とするマーク端末装置。

【請求項9】 印影または署名を表すマークによりデジタルデータの認証を行うマーク端末装置において、デジタルデータに付加されたマークからデジタルデータ認証情報を抽出して復号鍵により復号化し、マークが付加されているデジタルデータから特徴情報を抽出し、前記デジタルデータから抽出した特徴情報とマークから抽出したデジタルデータ認証情報中の特徴情報とを比較照合し、特徴情報が合致している場合には前記デジタルデータ認証情報の表示を行い、合致していない場合にはエラーメッセージを表示するマーク認証処理部を備えることを特徴とするマーク端末装置。

【請求項10】 前記マーク認証処理部は、認証処理でエラーが発生した場合に当該マークを無効なデザインに変更するものであることを特徴とする請求項8または請求項9のいずれかに記載されたマーク端末装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はデジタルデータを電子的なマークにより認証する電子マーク認証システムに関し、特にデジタルデータを印影や署名を表す電子マークにより認証する電子マーク認証システムに適用して有効な技術に関するものである。

【0002】

【従来の技術】ネットワーク上での商取引等が広がりつつある現在、伝達する情報の確からしさをネットワーク上で確認できる技術が重要になってきている。第3者が成りすましていないかを確認する本人認証については、「CardWave '98年3月号」でECOM（電子商取引実証推進協議会）の本人認証技術検討Gが各種の方式を分類しており、パスポートやクレジットカード等による所有物を利用する方式、指紋、声紋や筆跡等のバイオメトリクスを利用する方式、パスワードやデジタル署名等の秘密情報を利用する方式等があるが、ネットワークで用いる場合には所有物や秘密情報を用いる方式が一般的である。

【0003】また、情報の途中改ざんの確認については、インターネットを利用したEC(Electronic Commerce)で、クレジット決済を安全に行う為に用いられるSET(Secure Electronic Transactions)では、デジタル署名によるカード所有者の認証を行っている。デジタル署名は、通常伝達したい情報を圧縮した圧縮文を送り手

(3) 000-138671 (P2000-138671A)

の暗号鍵で暗号化した暗号文であり、送り手の復号鍵（公開鍵）で元の圧縮文に復号化できる。つまり、受け手は受け取ったメッセージから作った圧縮文と受け取ったデジタル署名から復号化した圧縮文とを比較することで、メッセージが改ざんされていないかの確認、つまり文書認証ができる。

【0004】一方、印鑑や署名が一般的に持つ意味合いは、本人認証と文書認証を合わせ持つと考えられる。従来の印鑑を電子化した電子印鑑システムはいくつか製品化されている。これらの製品により、社内での決済文書等において、印影イメージを用いて承認を行うことができる。中にはID管理による押印時のセキュリティ管理や、サーバでの押印履歴管理による不正コピー防止の機能を提供する製品もある。また特開平10-11509号公報の様に、印鑑やサイン等を文書に付加し、その形等を文書の特徴量で変形させ、その認証を可能にすることにより、文書の改ざんを防止することも考えられている。

【0005】

【発明が解決しようとする課題】デジタル署名は文書認証と本人認証の両方の機能を有するとも言えるが、文書等のデジタルデータの受け手はそのデジタルデータを見ただけでは、情報の正当性や送り手の確認をすることはできない。現実社会では実印の押印の様に見て確認できるものによって安心感を感じることがあるが、デジタル署名はこの様な視認性を持たないと言える。

【0006】一方、従来の電子印鑑システムでは目で見て確認できる印影を用いるが、印影自体は単なるデザインであって、文書等デジタルデータの受け手が送り手を確認するにはログ情報等の履歴を調べる必要があった。

【0007】また特開平10-11509号公報に記載された技術においても印影自体は単なるデザインデータであって、文書認証を行う為にはサーバ上の基準となる印影と文書の特徴量で変形させた印影とを比較する必要がある。つまり、例えば特定のイントラネット内におけるオンラインでの本人認証や文書認証はできるが、企業間のネットワーク、例えばエクストラネット等でのデジタルデータのやり取りにおいて、デジタルデータの受け手が、表示されたデジタルデータ上でその内容や送り手の確認をすることができる機能を備えている電子印鑑システムはなかったと言える。

【0008】また、従来のシステムの印影デザインは定型デザインの中から選ぶものである。つまり、例えば実社会で使用している印鑑やサインのデザインを印鑑システム上で使用することはできなかった。更に、視認性のある従来の電子印鑑システムとデジタル署名の両者を併用することは可能だが、それぞれを管理、運用する為には利用者・運用者共に煩雑な手順が必要となる。

【0009】本発明の目的は上記問題を解決し、ネットワーク上でデジタルデータを送受信する際の本人認証及

びデータ認証を実現することが可能な技術を提供することにある。

【0010】

【課題を解決するための手段】印影または署名を表すマークによりデジタルデータの認証を行う電子マーク認証システムにおいて、マークデザインに本人認証情報及びデジタルデータ認証情報を埋め込んだマークをデジタルデータに付加し、マーク中の認証情報を用いて当該デジタルデータの認証を行うものである。

【0011】本発明のマーク端末装置のマーク登録処理部が電子印鑑等のマークの新規登録または更新を要求するマーク登録要求をマーク管理サーバに送信すると、マーク管理サーバのマーク管理処理部は、マーク登録要求を受信し、要求元の人物を認証する為の情報を暗号鍵で暗号化した本人認証情報を当該要求元の印影デザイン等のマークデザインに埋め込んでマークを作成し、前記作成したマークに前記本人認証情報を復号化する為の復号鍵を添付して要求元に配布する。

【0012】またマーク管理サーバのマーク復号鍵管理処理部は、前記暗号化した本人認証情報を復号化する為の復号鍵をマーク復号鍵管理DBに登録し、前記登録した復号鍵を各マーク端末装置に送信する。

【0013】マーク端末装置のマーク登録処理部は、マーク管理サーバのマーク管理処理部から送信されたマークを受け取り、また各マーク端末装置の復号鍵格納処理部は、マーク復号鍵管理処理部から送信された復号鍵を受信して復号鍵DBに格納する。

【0014】マーク端末装置のマーク付加処理部は、マークが付加される文書等のデジタルデータについて、その特徴情報を含むデジタルデータ認証情報とマーク付加通算番号とをユーザ固有の暗号鍵で暗号化し、当該デジタルデータを送信するユーザの本人認証情報が埋め込まれたマークに前記暗号化されたデジタルデータ認証情報及びマーク付加通算番号を埋め込み、前記デジタルデータの選択された位置に前記マークを付加する。

【0015】前記の様にマークが付加されたデジタルデータが他のユーザのマーク端末装置に送信されると、そのマーク端末装置のマーク認証処理部は、デジタルデータに付加されたマークから本人認証情報を抽出し、その本人認証情報を復号化する為に添付された復号鍵が復号鍵DBに格納されている復号鍵と合致するかどうか照合し、前記復号鍵が合致している場合には前記マークから抽出した本人認証情報を前記復号鍵で復号化して本人認証情報を表示し、合致していない場合にはエラーメッセージを表示する。

【0016】またマーク端末装置のマーク認証処理部は、デジタルデータに付加されたマークからデジタルデータ認証情報を抽出して復号鍵により復号化し、マークが付加されているデジタルデータから特徴情報を抽出し、前記デジタルデータから抽出した特徴情報とマーク

(4) 000-138671 (P2000-138671A)

から抽出したデジタルデータ認証情報中の特徴情報とを比較照合し、特徴情報が合致している場合には前記デジタルデータ認証情報の表示を行い、合致していない場合にはエラーメッセージを表示する。

【0017】以上の様に本発明の電子マーク認証システムによれば、本人認証情報及びデジタルデータ認証情報を埋め込んで作成したマークをデジタルデータに付加し、マーク中の認証情報を用いて当該デジタルデータの認証を行うので、ネットワーク上でデジタルデータを送受信する際の本人認証及びデータ認証を実現することが可能である。

【0018】

【発明の実施の形態】以下に企業イントラネット及び企業間ネットワークにおいて電子印鑑を用いて本人認証及び文書認証を行う一実施形態の電子マーク認証システムについて説明する。

【0019】図1は本実施形態の電子印鑑認証システムの概略構成を示す図である。本実施形態の電子印鑑認証システムは、印鑑マークを管理する複数のシステム管理者100A～システム管理者100B（以下、単にシステム管理者100とも称する）と、複数の社員110A～社員110B（以下、単に社員110とも称する）が利用するシステムであって、図1に示す様に印鑑マーク管理サーバ101A（以下、単に印鑑マーク管理サーバ101とも称する）と、社員端末111A（以下、単に社員端末111とも称する）とが、企業イントラネット等の通信網120A（以下、単に通信網120とも称する）を介して互いに接続されて構成されている。これにインターネット等を経由して他社の同様のシステム或いはクライアント端末が接続される。なおここでいう印鑑マークとは、視認性のある画像データであって、印鑑を押印する本人に第3者が成りすましていないかの検証（以下、単に本人認証とも称する）及び印鑑を押印された文書等のデジタルデータが改ざんされていないかの検証（以下、単に文書認証とも称する）を行う為の、印鑑やサイン等のイメージデザインの形状をとるマークを示すものとする。

【0020】印鑑マーク管理サーバ101は、システム管理者100が管理する企業イントラネットや企業間のネットワーク取引で本人認証や文書認証を行うマーク管理サーバである。印鑑マーク管理サーバ101は、社員110の要求に応じて、各自の本人認証に必要な情報を埋め込んだ印鑑マークを作成し、後述の印鑑マーク管理DBに登録する。この時、印鑑マークのデザインは社員110が自由に作成できるが、不正な登録を防ぐ為に社員ID等で要求元の確認を行う。

【0021】社員端末111は社員110が利用するマーク端末装置である。社員110は、社員端末111を使ってビジネスに必要な文書等を作成したり、システム管理者100とデータのやり取りをしたりする。各自の

印鑑マークは社員端末111等で管理される。所属等の情報変更時にはシステム管理者100が印鑑マークの更新を行い、更新した印鑑マークを社員端末111に送信する。画面イメージ112は、印鑑マーク付きのデジタルデータを表示した時の画面表示例である。

【0022】図2は本実施形態の印鑑マーク管理サーバ101の概略構成を示す図である。図2に示す様に本実施形態の印鑑マーク管理サーバ101は、印鑑マーク管理処理部221と、印鑑マーク公開鍵管理処理部222とを有している。

【0023】印鑑マーク管理処理部221は、印鑑マークの新規登録または更新を要求するマーク登録要求を社員端末111から受信し、要求元の人物を認証する為の情報を秘密鍵で暗号化した本人認証情報を当該要求元の印影デザインに埋め込んで印鑑マークを作成し、前記作成した印鑑マークに前記本人認証情報を復号化する為の公開鍵を添付して要求元に配布するマーク管理処理部である。

【0024】印鑑マーク公開鍵管理処理部222は、暗号化した本人認証情報を復号化する為の公開鍵を印鑑マーク公開鍵管理DB211に登録し、前記登録した公開鍵を各社員端末111に送信するマーク復号鍵管理処理部である。

【0025】印鑑マーク管理サーバ101を印鑑マーク管理処理部221及び印鑑マーク公開鍵管理処理部222として機能させる為のプログラムは、CD-ROM等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する媒体はCD-ROM以外の他の媒体でも良い。

【0026】図2に示す様に本実施形態の印鑑マーク管理サーバ101は、表示装置201と、入力装置202と、通信網インタフェース203と、印鑑マーク管理DBインタフェース204と、印鑑マーク公開鍵管理DBインタフェース205と、印鑑マークログ管理DBインタフェース206と、記憶装置207と、CPU208と、メモリ209とがバス200によって互いに接続されて構成されている。また外部記憶装置として印鑑マーク管理DB210、印鑑マーク公開鍵管理DB211及び印鑑マークログ管理DB212が接続されている。

【0027】表示装置201は、印鑑マーク管理サーバ101を使用するシステム管理者100にメッセージ等を表示する為に用いられるものであり、CRTや液晶ディスプレイ等で構成される。入力装置202は、印鑑マーク管理サーバ101を使用するシステム管理者100がデータや命令等を入力する為に用いられるものであり、キーボードやマウス等で構成される。通信網インタフェース203は、通信網120を介して、社員端末111や他社の印鑑マーク管理サーバ101B等とデータのやり取りを行う為のインタフェースである。

(5) 000-138671 (P2000-138671A)

【0028】印鑑マーク管理DBインタフェース204は、印鑑マーク管理DB210とデータのやり取りを行う為のインタフェースである。印鑑マーク管理DB210は、社員ID、印鑑ID、印影等といったデータを対応付けて管理するものであり、例えば図4の様なものである。

【0029】印鑑マーク公開鍵管理DBインタフェース205は、印鑑マーク公開鍵管理DB211とデータのやり取りを行う為のインタフェースである。印鑑マーク公開鍵管理DB211は、取引のある企業の情報システム管理部署等の印鑑マーク管理者と本人認証用の公開鍵等といったデータを対応付けて管理するものであり、例えば図5の様なものである。

【0030】印鑑マークログ管理DBインタフェース206は、印鑑マークログ管理DB212とデータのやり取りを行う為のインタフェースである。印鑑マークログ管理DB212は、社員端末111でデジタルデータに印鑑マークを押印する時に該印鑑マークに埋め込む文書認証データを対応付けて管理するものであり、例えば図7の様なものである。

【0031】記憶装置207は、印鑑マーク管理サーバ101等で使用されるプログラムやデータを永続的に記憶する為に用いられるものであり、ハードディスクやフロッピーディスク等で構成される。

【0032】CPU208は、印鑑マーク管理サーバ101を構成する各部を統括的に制御したり、様々な演算処理を行ったりする。メモリ209には、OS220や印鑑マーク管理処理部221、印鑑マーク公開鍵管理処理部222といった、CPU208が上記の処理をする為に必要なプログラム等が一時的に格納される。ここでOS220は、印鑑マーク管理サーバ101全体の制御を行う為にファイル管理やプロセス管理或いはデバイス管理といった機能を実現する為のプログラムである。

【0033】印鑑マーク管理処理部221は、社員端末111から印鑑マーク登録/変更要求があった場合に第三者からの不正な要求でないかを確認する処理、登録すると判定した場合に、送付された印影デザインまたは印鑑マーク管理DB210で管理している印影デザインに本人情報を埋め込む処理、処理に基づいて印鑑マーク管理DB210を更新する処理、要求元に印鑑マークを送信する処理及び印鑑マーク押印時に送信されるログ情報を印鑑マークログ管理DB212に格納する処理を行う処理部である。

【0034】また印鑑マーク管理DB210は、権限を有した者のみが更新できるものとする。なお印影デザインに埋め込む本人情報は図6の様なものである。画像データの中に特定の情報を埋め込む技術は、「電子透かし」として知られている。「電子透かし」の技術については日経エレクトロニクス1997年683号の100ページから107ページに記載されている。人間の目で

は判別できない様に情報を埋め込む不可視透かしと、人間の目にも見える形で情報を埋め込む可視透かしがあり、不可視透かしの場合埋め込む情報量に限界があると言われている。印鑑マークの場合、印鑑イメージが象徴する意味が分かる範囲、つまりそのマークが何を表すかが分かる範囲であれば、多少デザインを変更しても支障がないので、図8の様に可視透かしと不可視透かしを組み合わせ、ある程度多くの情報を埋め込むことができる。

【0035】印鑑マーク公開鍵管理処理部222は、社外のデジタル文書に押印された印鑑マークの送手の確認、つまり本人認証を行う為に必要な公開鍵を印鑑マーク公開鍵管理DB211に登録・管理する処理、新しい公開鍵が印鑑マーク公開鍵管理DB211に登録されたら社員端末111等に接続している公開鍵DBに該公開鍵を送信する処理、及び公開鍵の送信要求があった場合には要求元に該公開鍵を送信する処理を行う処理部である。なお社外から公開鍵を受け取る場合は、企業のシステム管理者100に第三者が成りすますことを防止する為に、発信元の身元確認を行った上でFD等に格納した公開鍵を受け取るものとする。

【0036】図3は本実施形態の社員端末111の概略構成を示す図である。図3に示す様に本実施形態の社員端末111は、印鑑マーク登録処理部312と、印鑑マーク押印処理部313と、印鑑マーク認証処理部314と、公開鍵格納処理部315とを有している。

【0037】印鑑マーク登録処理部312は、印鑑マークの新規登録または更新を要求するマーク登録要求を印鑑マーク管理サーバ101に送信し、要求元の人物を認証する為の情報を秘密鍵で暗号化した本人認証情報を当該要求元の印影デザインに埋め込んで作成した印鑑マークを印鑑マーク管理サーバ101から受け取るマーク登録処理部である。

【0038】印鑑マーク押印処理部313は、印鑑マークが付加される文書の特徴情報を含む文書認証情報と押印通算番号とをユーザ固有の秘密鍵で暗号化し、本人認証情報が埋め込まれた印鑑マークに前記暗号化された文書認証情報及び押印通算番号を埋め込み、前記文書の選択された位置に前記印鑑マークを付加するマーク付加処理部である。

【0039】印鑑マーク認証処理部314は、文書に付加された印鑑マークから本人認証情報を抽出し、その本人認証情報を復号化する為に添付された公開鍵が公開鍵DB309に格納されている公開鍵と合致するかどうか照合し、前記公開鍵が合致している場合には前記印鑑マークから抽出した本人認証情報を前記公開鍵で復号化して本人認証情報を表示し、合致していない場合にはエラーメッセージを表示する本人認証処理と、文書に付加された印鑑マークから文書認証情報を抽出して公開鍵により復号化し、印鑑マークが付加されている文書から特徴

(6) 000-138671 (P2000-138671A)

情報を抽出し、前記文書から抽出した特徴情報と印鑑マークから抽出した文書認証情報中の特徴情報とを比較照合し、特徴情報が合致している場合には前記文書認証情報の表示を行い、合致していない場合にはエラーメッセージを表示するデータ認証処理とを行うマーク認証処理部である。公開鍵格納処理部315は、本人認証情報を復号化する為の公開鍵を印鑑マーク管理サーバ101から受信し、前記公開鍵を公開鍵DB309に格納する復号鍵格納処理部である。

【0040】社員端末111を印鑑マーク登録処理部312、印鑑マーク押印処理部313、印鑑マーク認証処理部314及び公開鍵格納処理部315として機能させる為のプログラムは、CD-ROM等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する媒体はCD-ROM以外の他の媒体でも良い。

【0041】図3に示す様に本実施形態の社員端末111は、表示装置301と、入力装置302と、通信網インタフェース303と、公開鍵DBインタフェース304と、記憶装置305と、CPU306と、メモリ307とがバス300によって互いに接続されて構成されている。また印影デザインとして従来実社会で使用している印鑑のデザインを利用する場合には、イメージスキャナ308を接続して使用したいデザインをビットマップ等で読み込んだ後に編集できる様にする。

【0042】表示装置301は、社員端末111を使用する社員110にメッセージ等を表示する為に用いられるものであり、CRTや液晶ディスプレイ等で構成されている。入力装置302は、社員端末111を使用する社員110がデータや命令等を入力する為に用いられるものであり、キーボードやマウス等で構成される。通信網インタフェース303は、通信網120を介して、印鑑マーク管理サーバ101や社員端末111B等とデータのやり取りを行う為のインタフェースである。

【0043】公開鍵DBインタフェース304は、公開鍵DB309がある場合にデータのやり取りを行う為のインタフェースである。記憶装置305は、社員端末111等で使用されるプログラムやデータを永続的に記憶する為に用いられるものであり、ハードディスクやフロッピーディスク等で構成される。

【0044】CPU306は、社員端末111を構成する各部を統括的に制御したり、様々な演算処理を行ったりする。メモリ307には、OS310や、グループウェアシステム等311、印鑑マーク認証処理部314、印鑑マーク情報記憶部316といった、CPU306が上記の処理をする為に必要なプログラム等が一時的に格納される。ここでOS310は、社員端末111全体の制御を行う為にファイル管理やプロセス管理或いはデバイス管理といった機能を実現する為のプログラムである。グループウェアシステム等311は、社員端末111

1が社内外とデジタルデータをやり取りし、必要なデータを表示する為のシステムで、デジタルデータに押印された認証情報を扱う為に、印鑑マーク認証処理部314とのインタフェースを持つ。なおこのグループウェアシステム等311の部分は、デジタルデータをハンドリングするアプリケーションシステムであれば、どの様なものでも良く、特にグループウェアシステムに限定するものではない。また、直接印鑑マーク認証処理部314を個別アプリケーションシステムとしてOS310上で動かす場合もある。

【0045】印鑑マーク登録処理部312は、印鑑マーク登録の為の印影デザインを作成する処理、印鑑マーク管理サーバ101に印鑑マーク登録要求を送信する処理及び印鑑マーク管理サーバ101から送信された印鑑マークを受信する処理を行う。

【0046】印鑑マーク押印処理部313は、社員110が社員端末111でデジタルデータに電子印鑑を押印する為の処理で、必要なデジタルデータを表示し、社員IDに対応するパスワードが入力されたら、該社員IDに対応する印鑑マークを呼び出す処理、選択された文書認証情報と印鑑マークの押印通算番号等の押印時情報を固有の秘密鍵で暗号化したものを印鑑マークの特定のブロックに埋め込む処理及び文書の指定された位置に印鑑マークを押印する処理等を行う。

【0047】印鑑マーク認証処理部314は、社員110が社員端末111で受信したデジタルデータの送り手や内容の認証を行う為の処理部である。必要なデジタルデータを表示し、選択された認証項目に対応して、印鑑マークに埋め込まれた本人認証情報を予め印鑑マーク管理サーバ101より配布された公開鍵で復号化して表示する本人認証処理、印鑑マークに埋め込まれた文書認証情報を印鑑マークに添付された公開鍵で復号化して表示する文書認証処理、前記公開鍵で復号化できない場合にエラーメッセージを表示する処理及び表示したデジタルデータの有効期限やファイル名等の情報をチェックし、無効と判断される場合は印影を無効なデザインに変形させる処理等を行う。

【0048】印鑑マーク情報記憶部316は、印鑑マーク認証処理部314によって社員端末111で呼び出した印鑑マークや公開鍵を一時的に格納するものである。なお企業間でネットワーク取引を行う等、本人認証情報の確認の為に必要な公開鍵が複数必要な場合は、公開鍵DB309を社員端末111或いは通信網120に接続し、印鑑マーク公開鍵管理DB211から必要な公開鍵を公開鍵DBインタフェース304に送信し、社員端末111から参照できる様にする。また企業イントラネット内でのみ印鑑マークを用いる場合は、予め社員端末111に公開鍵を持たせておいても良く、公開鍵の格納方法は限定しない。

【0049】図4は本実施形態の印鑑マーク管理DB2

!(7) 000-138671 (P2000-138671A)

10のデータ例を示す図である。社員ID401、印鑑ID402、氏名403、メールアドレス404、所属・役職他の情報405、印影データ406等を一定の表記基準に基づいて表記を統一して格納する。新しい印鑑マークを登録したり、既存の印鑑マークの所属・役職他の情報405を変更した際等に印鑑マーク管理DB210を更新する。

【0050】図5は本実施形態の印鑑マーク公開鍵管理DB211のデータ例を示す図である。データ番号501、印鑑マーク管理者502、管理者アドレス503、公開鍵データ504等を一定の表記基準に基づいて表記を統一して格納する。印鑑マーク公開鍵管理DB211は、本人認証の為に公開鍵データ504を管理するDBであり、新たに印鑑マークを利用する企業が増えたり、公開鍵データ504の変更があった際等に印鑑マーク公開鍵管理DB211を更新する。なお予め公開鍵データ504の有効期限等が設定されている場合はそのデータも管理する。

【0051】図6は本実施形態の本人認証データの例を示す図である。図6では印鑑マーク管理サーバ101において印鑑マーク管理処理部221が、社員110の要求に応じて印影に本人認証情報を埋め込む際の本人認証データの例を表している。印鑑ID601、氏名602、メールアドレス603、所属・役職他604等を、印鑑マーク管理サーバ101の印鑑マーク管理処理部221によって印鑑マーク管理サーバ101で管理する秘密鍵で暗号化して印鑑マークのエンティティとして埋め込む。埋め込む際には、例えば図8の印影イメージ802の様に、印影の氏名部分に不可視透かしで埋め込み、可視透かしの形で会社名を埋め込む。つまり、予め印影の中を2つ以上のブロックに区分し、特定のブロックに本人認証情報を埋め込む。なお社印の様な印鑑においては、押印の責任部署を本人認証情報として用いる場合もある。

【0052】図7は本実施形態の文書認証データの例を示す図である。図7では社員端末111において社員110がデジタルデータに印鑑マークを押印する際に文書認証情報として埋め込まれる文書認証データの例を表している。社員端末111の印鑑マーク押印処理部313は、印鑑ID701、印鑑マーク押印通算NO. 702、作成日時703、有効期限704、ファイル名705、端末ID706、押印したいデジタルデータの特徴情報707等を印鑑マーク押印処理部313が管理する秘密鍵によって社員端末111で暗号化して印鑑マークのエンティティとして埋め込む。例えば図8の印影イメージ803の様に、本人認証情報を埋め込んだブロック以外の印影の周辺部分に文書認証情報の埋め込みを行う。デジタルデータの特徴情報707としては、文字データのコードを数値とみなして加算した、いわゆるチェックサムと呼ばれるものやデジタルデータの内容の圧縮

文等を用いる。

【0053】また図7は印鑑マークログ管理DB212のデータ例でもある。社員端末111の印鑑マーク押印処理部313によって、図7の様なデータを押印時のログ情報として印鑑マーク管理サーバ101に送信し、印鑑マーク管理処理部221によって該ログ情報を印鑑マークログ管理DB212に格納する。なお本人認証及び文書認証に必要なデータは、図6及び図7の例に限らず、ISO9001の認証を取得する際の電子データの記録情報として必要な情報を満たすものとする。

【0054】図8は本実施形態の印影及び印鑑マークのイメージ例を示す図である。例えば印影イメージ801の様な印影に、本人認証情報を埋め込む。この時、予め印影の中を2つ以上のブロックに区分し、各々特定のブロックに本人認証情報や文書認証情報を埋め込むことにする。例えば、印影イメージ802の様に氏名部分と可視透かしの会社名部分に、本人認証情報を埋め込み、印影イメージ803の様な印影の周辺部分に文書認証情報を埋め込むといったブロック区分を行い、社員端末111の印鑑マーク認証処理部314で認証情報を復号化するには、対応するブロックから埋め込まれた情報が自動的に抽出される様にする。なお印影イメージ801では、印影デザイン例として個人の認め印のデザインを用いたが、日付入りの職印やサイン等のデザインでも良いし、また社印として用いる際には企業名等でも良く、印影イメージ801の印影デザイン例に限定するものではない。但し単なるイメージデザインと異なり、認証情報が埋め込まれていると感じられる様な信頼感を与える印影デザインであることが重要である。

【0055】次に本実施形態の電子印鑑認証システムの動作について説明する。図9は本実施形態の初期画面のイメージ例を示す図である。図9では社員端末111によって表示される電子印鑑認証システムの初期画面イメージ例を表している。初期画面900は、必要なデジタル文書等を表示するデジタルデータ表示エリア901と、印鑑マークの機能アイコンが並ぶ印鑑マーク機能表示エリア902と、OK、キャンセル、ファイルといった基本機能のアイコンが並ぶ基本機能表示エリア903により構成される。但し初期画面900は各エリアの配置例であり、この配置に限定するものではない。

【0056】図10は本実施形態の印鑑マーク登録処理の処理手順を示すフローチャートである。図10では社員端末111と印鑑マーク管理サーバ101との間で印鑑マークの登録を行う処理フローを表している。まず社員110が、図9の様な初期画面900の印鑑マーク機能表示エリア902の登録ボタンをクリックすると、印鑑マーク登録処理部312は、印鑑マークの登録要求を印鑑マーク管理サーバ101に送信する（ステップ1001）。印鑑マーク登録要求を受信した印鑑マーク管理サーバ101は、印鑑マーク管理処理部221によ

(8) 000-138671 (P2000-138671A)

て、登録要求元の社員ID401を元に印鑑マーク管理DB210から要求元のメールアドレス404を読み出し、要求元のメールアドレス404に印鑑マーク要求／変更の確認依頼を送信する（ステップ1002及びステップ1003）。確認依頼を受信した社員端末111の印鑑マーク登録処理部312は、イメージスキャナ等を用いて作成した、登録或いは変更したい印影デザインを印鑑マークの要求確認結果と共に印鑑マーク管理サーバ101に送信する（ステップ1004及びステップ1005）。印影と印鑑マークの要求確認結果を受信した印鑑マーク管理サーバ101は、印鑑マーク管理処理部221を用いて、印鑑マーク管理サーバ101で管理する当該サーバの秘密鍵で本人認証情報を暗号化し、これを受信した印影デザインに埋め込んで印鑑マークを作成する（ステップ1008）。印鑑マーク管理DB210内の登録或いは変更した印鑑マークの情報を更新した後（ステップ1009）、その本人認証情報を復号する為の公開鍵と共に前記作成した印鑑マークを要求元の社員110にFD等で配布する（ステップ1010）。社員110は、配布された印鑑マークを社員端末111に格納する（ステップ1011及びステップ1012）。

【0057】図11は本実施形態の印鑑マーク押印処理の処理手順を示すフローチャートである。図11では社員端末111において文書認証情報を埋め込んだ印鑑マークを文書に押印する処理フローを表している。図12は本実施形態の図11の処理フローに対応する処理画面のイメージを示す図である。この図11及び図12と前述の図9を用いて、上記処理フローを説明する。まず社員110が、押印したい文書データ等を基本機能表示エリア903にあるファイルボタンにより選択し、デジタルデータ表示エリア901に表示する（ステップ1101）。印鑑マーク機能表示エリア902の印鑑マークの呼出ボタンをクリックすると、印鑑マーク押印処理部313によって、図12の処理画面イメージ1201の様な社員ID401とパスワードの入力欄が表示される（ステップ1102及びステップ1103）。印鑑マーク押印処理部313は、入力されたパスワードと予め社員端末111に格納されているパスワードとを照合し、合致しなかった場合はエラーメッセージを表示し、合致した場合は印鑑マーク欄に印鑑マークを表示する（ステップ1104～ステップ1106）。次に文書情報の埋め込みボタンをクリックすると、図12の処理画面イメージ1202の様に、印鑑マーク押印処理部313によって文書認証情報の項目欄を表示する（ステップ1107及びステップ1108）。必要な項目を選択してOKをクリックすると印鑑マーク押印処理部313は、選択された文書情報と押印通算番号を社員毎に予め決められた各社員に固有の秘密鍵で暗号化して印鑑マークに埋め込み、また、その復号化に必要な公開鍵を添付して印鑑マーク欄に該印鑑マークを表示する（ステップ1109

～ステップ1113）。押印位置を選択して印鑑マーク機能表示エリア902の押印ボタンをクリックすると印鑑マーク押印処理部313は、印鑑マークを文書の設定された位置に押印する（ステップ1114～ステップ1116）。なお文書認証情報の復号の為に必要な社員固有の公開鍵は、印鑑マークに添付せずに本人認証時に取得するものとしても良い。

【0058】図13は本実施形態の本人認証処理の処理手順を示すフローチャートである。図14は本実施形態の図13の処理フローに対応する処理画面のイメージ例を示す図である。まず社員端末111で図14の処理画面イメージ1401の様に印鑑マークが貼り付けられたデジタルデータを表示し、社員110が印鑑マークの認証ボタンをクリックすると、印鑑マーク認証処理部314は印鑑マークの認証項目欄を表示する（ステップ1301及びステップ1302）。図14の処理画面イメージ1402の様に社員110が印鑑マークの本人認証項目をクリックすると、印鑑マーク認証処理部314は、該印鑑マークから本人認証情報を抽出する（ステップ1303）。抽出した本人認証情報を復号化する為の公開鍵が、社員端末111或いは公開鍵DB309に格納してある公開鍵と合致するかどうか照合する（ステップ1305）。復号化する為の公開鍵が合致した場合に印鑑マーク認証処理部314は、該印鑑マークから抽出した本人認証情報を復号化して、内容を確認できる様に図14の処理画面イメージ1403の様に本人認証情報を表示し（ステップ1306）、合致しなければエラーメッセージを表示する（ステップ1307）。更に、エラーメッセージを表示した場合は、印影を消す、印影に×を付ける等、印鑑マークを無効なデザインに変形する（ステップ1308）。また本人認証情報として表示された内容を本人に確認したい場合は、本人認証情報の中のメールアドレス宛に確認依頼のメールを送信する。なお本人認証結果の表示方法は、図14の処理画面イメージ例に限定されるものではなく、例えばエラーメッセージは音声等によって表現しても良い。

【0059】図15は本実施形態の文書認証処理の処理手順を示すフローチャートである。なお文書認証処理フローの最初の工程で、本人認証処理フローと同じ部分、図13でいうとステップ1301及びステップ1302に相当する部分は省略した。図16は本実施形態の図15の処理フローに対応する処理画面のイメージ例を示す図である。まず社員110が、社員端末111で図16の処理画面イメージ1601の様に印鑑マークの文書認証項目をクリックする（ステップ1501）。印鑑マーク認証処理部314は、該印鑑マークから文書情報の復号化に必要な公開鍵と文書認証情報を抽出し、文書認証情報を復号化する（ステップ1502～ステップ1504）。次に該印鑑マークが押印されている文書等のデジタルデータから特徴情報を抽出し、該印鑑マークから抽

!(9) 000-138671 (P2000-138671A)

出した文書認証情報の中の特徴情報707と比較照合する(ステップ1505及びステップ1506)。この結果、合致しなかった場合は、文書等のデジタルデータが作成時点のものと異なることになるので、「このデータは変更されています」等のエラーメッセージを表示し、かつ印影を消す、印影に×を付ける等、印鑑マークを無効なデザインに変形する(ステップ1507及びステップ1508)。特徴情報707が合致した場合は更に有効期限等の情報を確認し、OKであれば図16のステップ処理画面イメージ1602の様に確認の為に文書情報の表示を行い(ステップ1509及びステップ1510)、有効期限704が切れている等の場合には、印影を消す、印影に×を付ける等、印鑑マークを無効なデザインに変形する(ステップ1508)。なお文書認証結果の表示方法は、図16の処理画面イメージ例に限定されるものではなく、例えばエラーメッセージの表示は音等でも良い。

【0060】印鑑マークの第3者による不正押印を防ぐ為にパスワードを用いているが、よりセキュリティを高める為に、例えばパスワードをIDカードで管理し、使用する時には印鑑マーク認証処理部314によってIDカードからパスワードを読み取る様にしても良い。この時、パスワードを予め暗号化しておくによりセキュリティが高くなる。

【0061】また本人認証情報のみが埋め込まれた他者の印鑑マークを不正入手し、自分の秘密鍵で文書情報を該印鑑マークに埋め込み、不正使用する等への対応策としては、例えば印鑑マークの押印通算NO. 702を利用する。社員端末111で文書認証情報を埋め込んだ印鑑マークを押印時に、押印通算NO. 702をログ情報として自動的に印鑑マーク管理サーバ101に送信し、印鑑マークログ管理DB212でログ情報を管理することで前述の様な不正が行われた際にチェックすることができる。

【0062】以上、本発明の実施形態について企業イントラネット及び企業間ネットワークの例を用いて説明したが、本発明はこの実施形態に限定されるものではない。例えば個人がネットワーク上で電子商取引を行う際に作成する注文書の様な、ネットワーク上でやり取りする一般的なデジタルデータに適用することも可能である。また従来印鑑証明を発行していた自治体が印鑑マーク管理機関になり、実印の印鑑登録時に、印鑑マークを申請した人に対してFD等で本人認証情報を埋め込んだ印鑑マークと印鑑マーク認証処理部314を配布する方法も考えられる。

【0063】以上説明した様に本実施形態の電子マーク認証システムによれば、本人認証情報及びデジタルデータ認証情報を埋め込んで作成したマークをデジタルデータに付加し、マーク中の認証情報を用いて当該デジタルデータの認証を行うので、ネットワーク上でデジタルデ

ータを送受信する際の本人認証及びデータ認証を実現することが可能である。

【0064】

【発明の効果】本発明によれば本人認証情報及びデジタルデータ認証情報を埋め込んで作成したマークをデジタルデータに付加し、マーク中の認証情報を用いて当該デジタルデータの認証を行うので、ネットワーク上でデジタルデータを送受信する際の本人認証及びデータ認証を実現することが可能である。

【図面の簡単な説明】

【図1】本実施形態の電子印鑑認証システムの概略構成を示す図である。

【図2】本実施形態の印鑑マーク管理サーバ101の概略構成を示す図である。

【図3】本実施形態の社員端末111の概略構成を示す図である。

【図4】本実施形態の印鑑マーク管理DB210のデータ例を示す図である。

【図5】本実施形態の印鑑マーク公開鍵管理DB211のデータ例を示す図である。

【図6】本実施形態の本人認証データの例を示す図である。

【図7】本実施形態の文書認証データの例を示す図である。

【図8】本実施形態の印影及び印鑑マークのイメージ例を示す図である。

【図9】本実施形態の初期画面のイメージ例を示す図である。

【図10】本実施形態の印鑑マーク登録処理の処理手順を示すフローチャートである。

【図11】本実施形態の印鑑マーク押印処理の処理手順を示すフローチャートである。

【図12】本実施形態の図11の処理フローに対応する処理画面のイメージ例を示す図である。

【図13】本実施形態の本人認証処理の処理手順を示すフローチャートである。

【図14】本実施形態の図13の処理フローに対応する処理画面のイメージ例を示す図である。

【図15】本実施形態の文書認証処理の処理手順を示すフローチャートである。

【図16】本実施形態の図15の処理フローに対応する処理画面のイメージ例を示す図である。

【符号の説明】

100…システム管理者、101…印鑑マーク管理サーバ、110…社員、111…社員端末、112…画面イメージ、120…通信網、200…バス、201…表示装置、202…入力装置、203…通信網インタフェース、204…印鑑マーク管理DBインタフェース、205…印鑑マーク公開鍵管理DBインタフェース、206…印鑑マークログ管理DBインタフェース、207…記

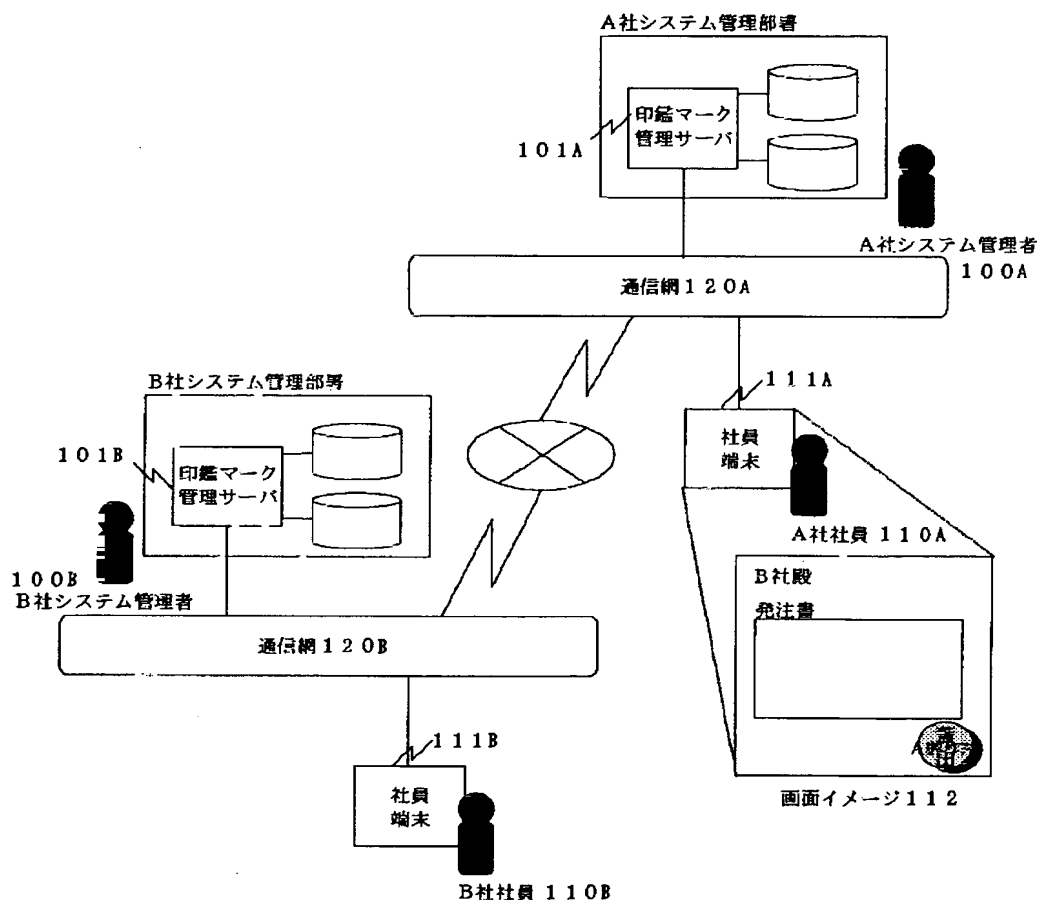
(図1) 00-138671 (P2000-138671A)

憶装置、208…CPU、209…メモリ、210…印鑑マーク管理DB、211…印鑑マーク公開鍵管理DB、212…印鑑マークログ管理DB、220…OS、221…印鑑マーク管理処理部、222…印鑑マーク公開鍵管理処理部、300…バス、301…表示装置、302…入力装置、303…通信網インタフェース、304…公開鍵DBインタフェース、305…記憶装置、306…CPU、307…メモリ、308…イメージスキャナ、309…公開鍵DB、310…OS、311…グループウェアシステム等、316…印鑑マーク情報記憶部、312…印鑑マーク登録処理部、313…印鑑マーク押印処理部、314…印鑑マーク認証処理部、315…公開鍵格納処理部、401…社員ID、402…印鑑ID、403…氏名、404…メールアドレス、405

…所属・役職他の情報、406…印影データ、501…データ番号、502…印鑑マーク管理者、503…管理者アドレス、504…公開鍵データ、601…印鑑ID、602…氏名、603…メールアドレス、604…所属・役職他、701…印鑑ID、702…通算NO.、703…作成日時、704…有効期限、705…ファイル名、706…端末ID、707…特徴情報、801～803…印影イメージ、900…初期画面、901…デジタルデータ表示エリア、902…印鑑マーク機能表示エリア、903…基本機能表示エリア、1201～1203…処理画面イメージ、1401～1403…処理画面イメージ、1601及び1602…処理画面イメージ。

【図1】

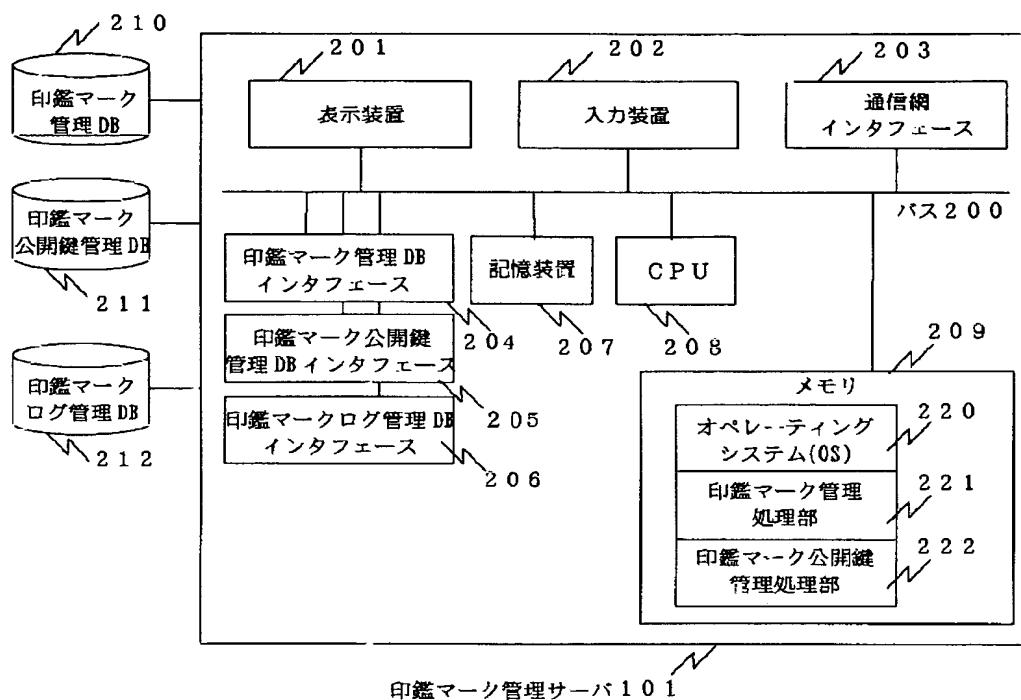
図1



(1) 100-138671 (P2000-138671A)



【図2】

図 2



【図4】

図 4

社員ID	印鑑ID	氏名	メールアドレス	所属・役職他	印影
D001101117	A00123	相川太郎	Aikawa@aa.co.jp	〇〇事業部 事業部長	
A035410506	A00124	藍田次郎	Aida@aa.co.jp	〇〇事業部 課長	
H001100402	-	愛野三郎	Aino@aa.co.jp	〇〇事業部 担当	-

【図6】

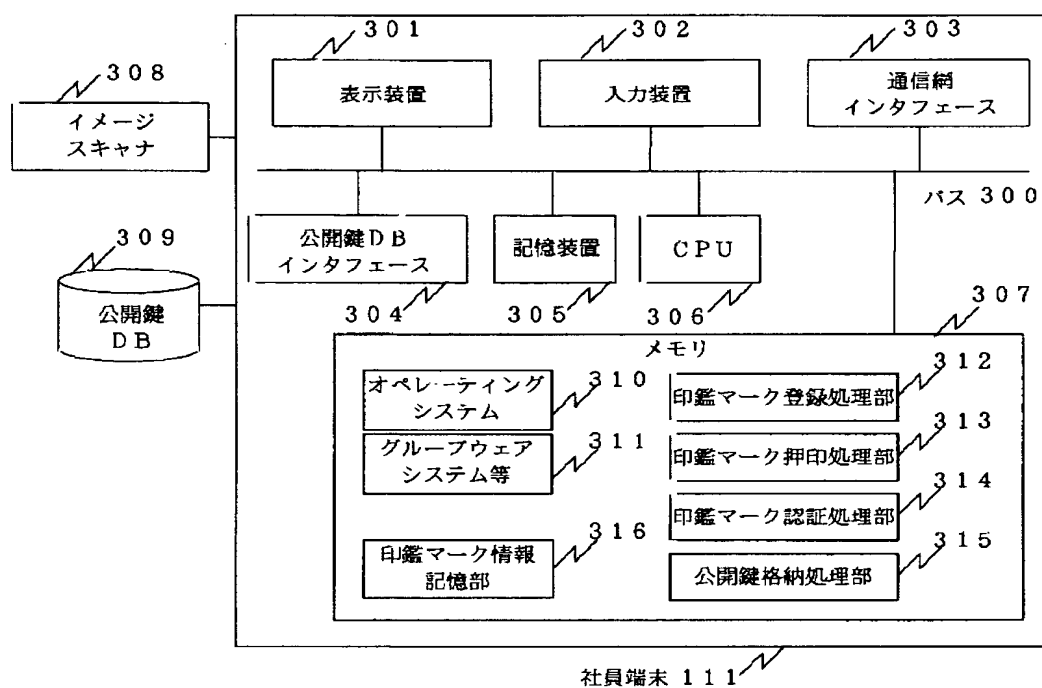
図 6

印鑑ID	氏名	メールアドレス	所属・役職他
A00123	相川太郎	Aikawa@aa.co.jp	〇〇事業部 事業部長

(株) 00-138671 (P2000-138671A)

【図3】

図 3



【図5】

図 5

501 NO	502 印鑑マーク管理者	503 管理者アドレス	504 公開鍵
1	A社印鑑マーク管理	im@aa.co.jp	pw*****gl*****qgm*
2	B社印鑑マーク管理	im@bb.co.jp	*ajk**yu*****aqz*r

【図7】

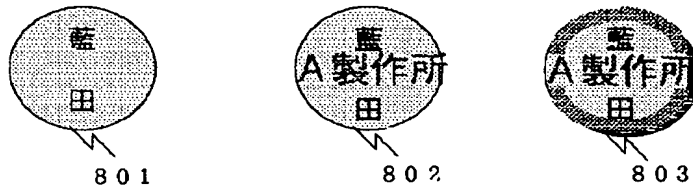
図 7

701 印鑑 ID.	702 通算 NO.	703 作成日時	704 有効期限	705 ファイル名	706 端末 ID	707 データの特徴情報
A00123	000089	1998.7.7	1998.12.31	158.2*/**.doc	PC792	*****

(13) 100-138671 (P2000-138671A)

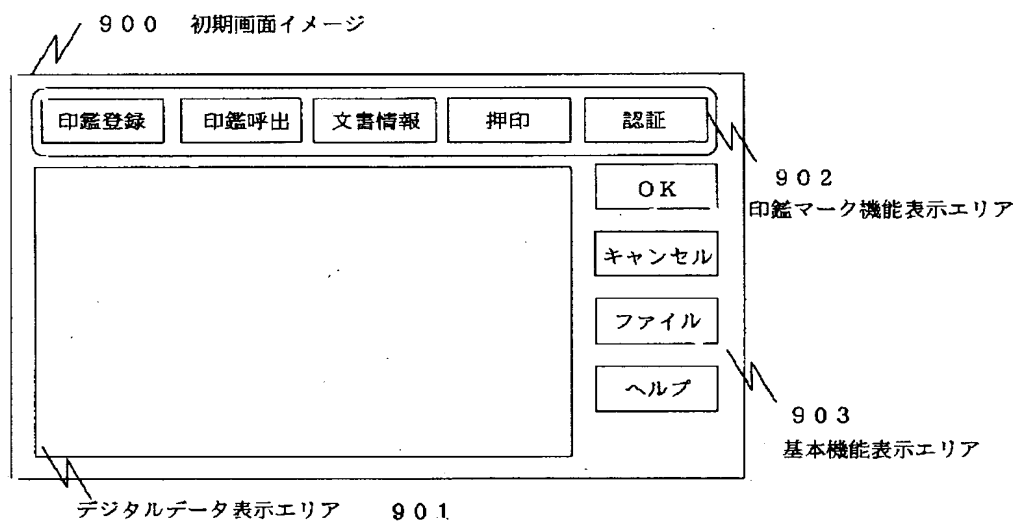
【図8】

図 8



【図9】

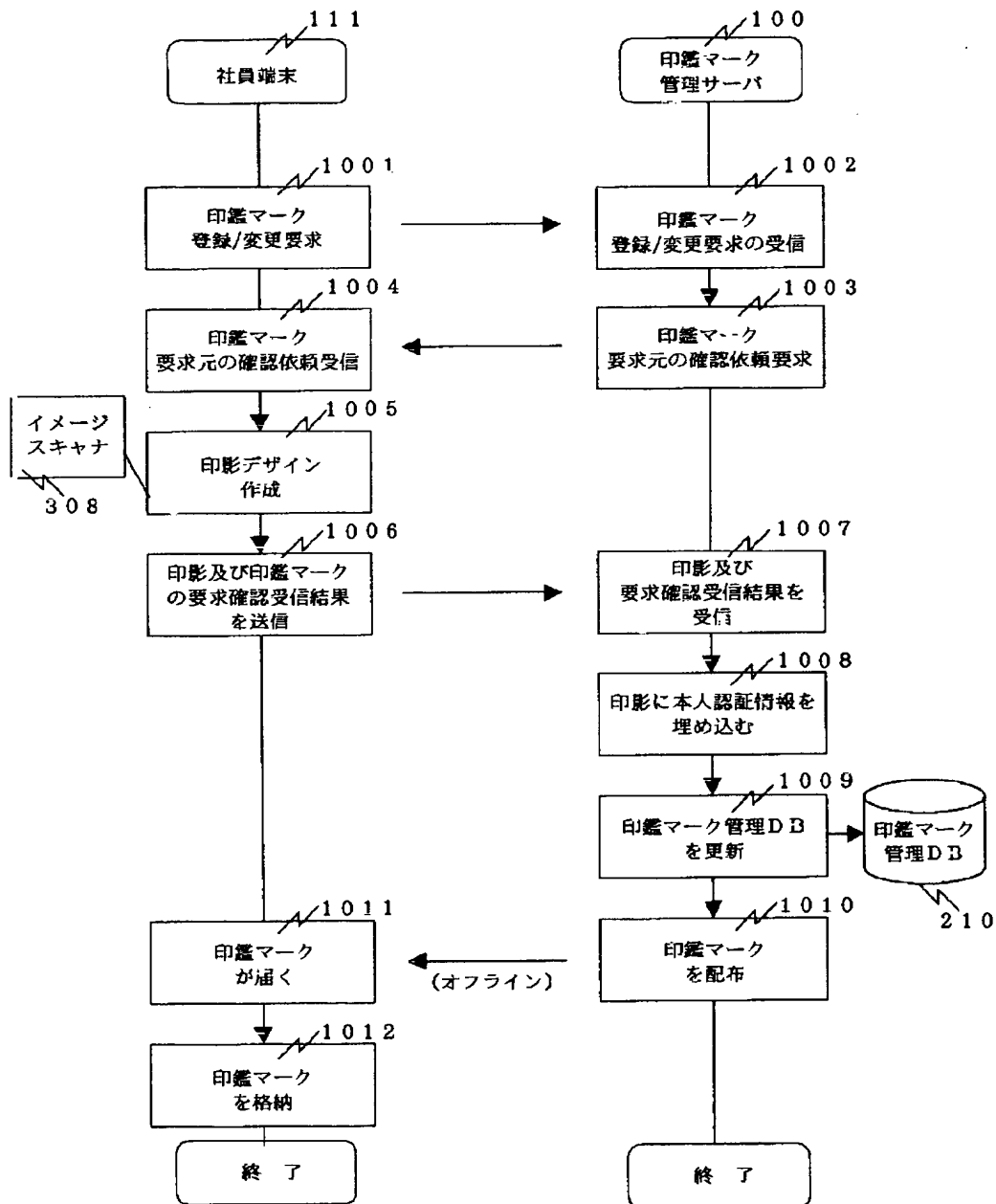
図 9



(4) 100-138671 (P2000-138671A)

【図10】

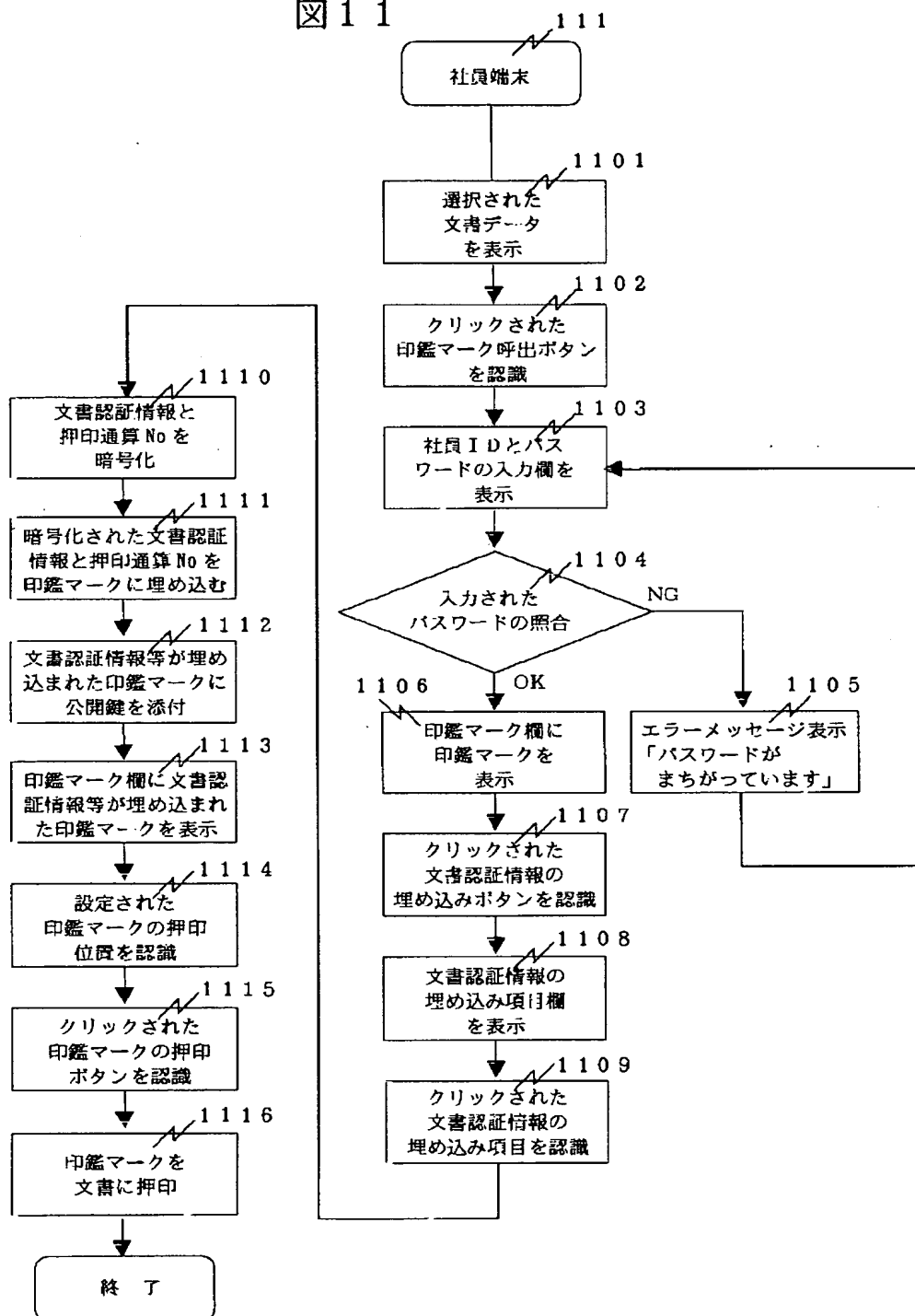
図10



(特 許) 100-138671 (P2000-138671A)

【図11】

図 11



(6) 00-138671 (P2000-138671A)

【図12】

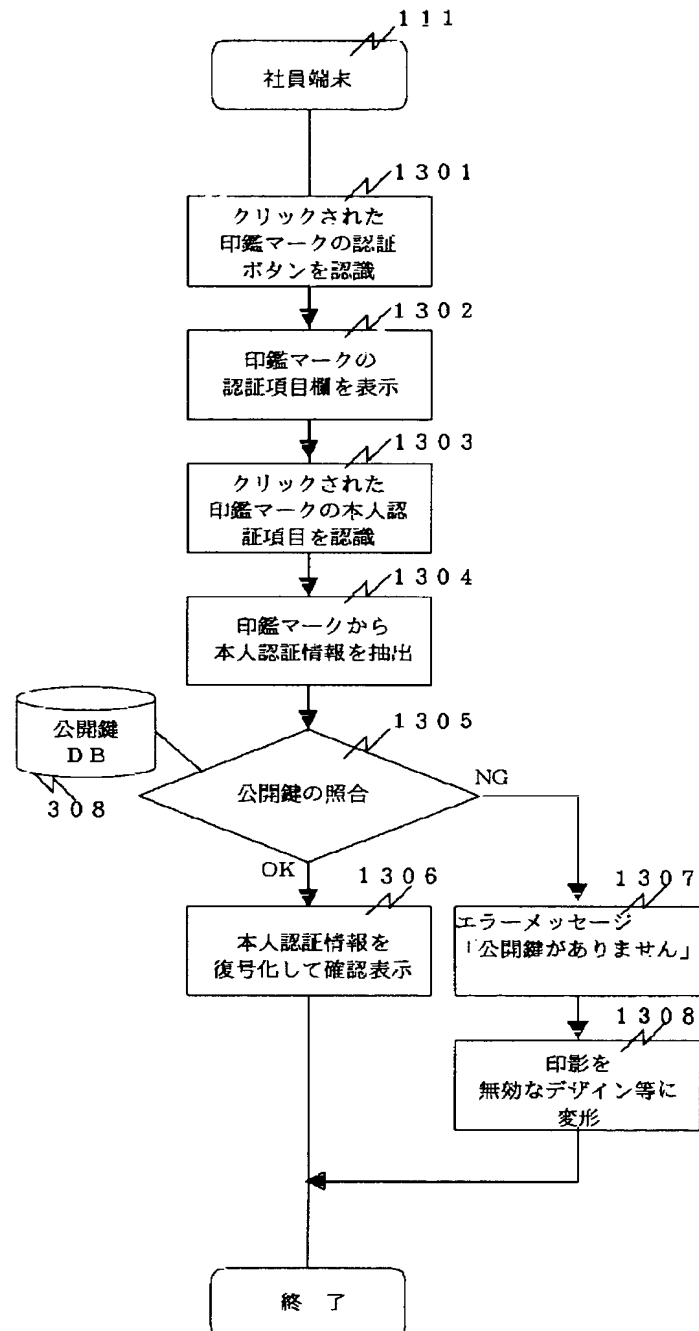
図 12

Figure 12 displays three screenshots of a software interface for stamp management:

- 1201:** A dialog box titled "印鑑マークの呼出" (Stamp Mark Callout). It contains fields for "ID" and "パスワード" (Password). Buttons include "OK", "キャンセル" (Cancel), "ファイル" (File), and "ヘルプ" (Help).
- 1202:** A dialog box titled "文書情報の入力" (Document Information Entry). It includes checkboxes for "タイトル" (Title), "作成日" (Creation Date), "ファイル名" (File Name), "有効期限" (Validity Period), and "文書の特徴情報" (Document Characteristics). It also has "OK" and "キャンセル" buttons.
- 1203:** A dialog box titled "〇〇システム発注書" (〇〇 System Order Form). It includes a checkbox for "印鑑マーク" (Stamp Mark) and a "+" button. It also has "OK", "キャンセル", "ファイル", and "ヘルプ" buttons.

【図13】

図 13



(株) 100-138671 (P2000-138671A)

【図14】

図14

Figure 14 shows three screenshots of a software interface for document registration. The first screenshot (1401) displays a 'Document Registration' window with a 'Stamp' button. The second screenshot (1402) shows a 'Stamp Confirmation' dialog box with checkboxes for 'Personal Information Confirmation' and 'Document Information Confirmation'. The third screenshot (1403) shows the 'Document Information Confirmation' dialog box with a list of document details including name, address, and email.

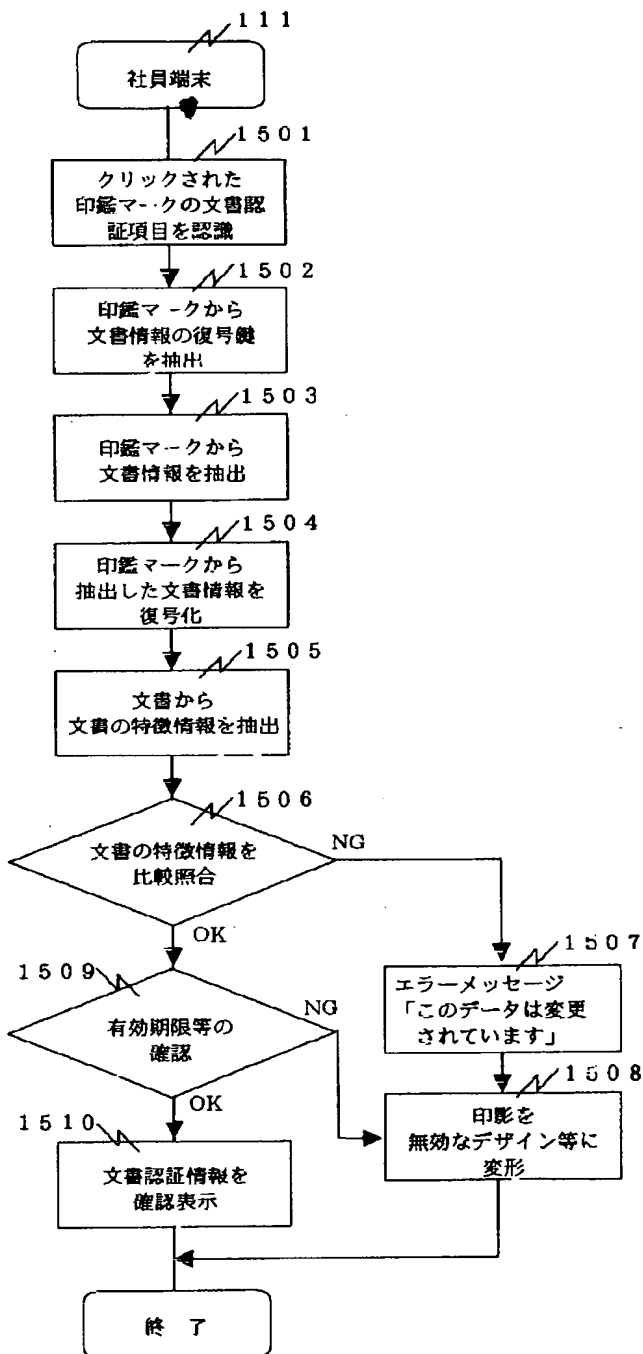
【図16】

図16

Figure 16 shows two screenshots of a software interface for document registration. The first screenshot (1601) displays a 'Stamp Confirmation' dialog box with checkboxes for 'Personal Information Confirmation' and 'Document Information Confirmation'. The second screenshot (1602) shows the 'Document Information Confirmation' dialog box with a list of document details including name, address, and email.

【図15】

図15



(8) 0 0 - 1 3 8 6 7 1 (P 2 0 0 0 - 1 3 8 6 7 1 A)

フロントページの続き

(51)Int.Cl. ⁷	識別記号	F I	(参考)
		H 0 4 L 9/00	6 7 5 D
(72)発明者 永井 康彦		Fターム(参考)	5B043 AA09 BA06 BA09 CA10 FA02
神奈川県川崎市麻生区王禅寺1099番地 株			FA03 FA07 FA08 GA18
式会社日立製作所システム開発研究所内			5B049 EE05 EE09 FF03 FF04 GG04
			GG07 GG10
			5J104 AA07 AA09 AA14 LA06 MA03
			PA07